UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,025	12/21/2005	Luis Barriga Caceres	P18155-US1	1351

27045 7590 11/24/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/595,025
Filing Date: 12/21/2005
Appellant(s): CACERES ET AL.

Roger S. Burleigh
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 08/18/2009 appealing from the Office action mailed 02/18/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

The amendment after final rejection filed on 04/20/2009 has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

The following is a listing of the evidence (e.g., patents, publication, Official Notice, and admitted prior art) relied upon in the rejection of claims under appeal.

6,643,782	Jin et al., (hereinafter "Jin"),	November 04, 2003.
6,571,289	Montenegro,	May 27, 2003.
6,105,027	Schneider et al., (hereinafter "Schneider")	August 15, 2000.

(9) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 24-27 and 29-40 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

- **Regarding claim 24**, the claim is directed to non-statutory subject matter.

Although the preamble of the claim recites *"an apparatus,"* the body of the claim does not positively recite any elements of hardware. The body of claim recites *"means for receiving the access credential," "means for checking validity of the access credential, "means for establishing a valid session," "means for assigning an internal IP address" "means for linking,"* and *"means for establishing a secure channel."* There is no further disclosure in the specification as to how the aforementioned "means for" are implemented. In light of discussions in the specification, *pars. 0023-0024 and 0065-0066 (accessing a local HTTP/non-HTTP services), par. 0048 (AAA protocol in accordance with IETF RFC*

2865 protocol), it appears reasonable that said "means for" are implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed subject matter is directed to non-statutory subject matter. The mere recitation of the machine in the preamble with an absence of a machine/hardware element in the body of the claim fails to make the claim statutory under 35 U.S.C 101. See ***In re Comiskey***, 499 F.3d 1365 (Fed. Cir. 2007); ***In Re Bilski***, 88 USPQ2d 1385; ***Diamond v. Diehr***, 450 U.S. 175, 184 (1981); ***Parker v. Flook***, 473 U.S. 584, 588 n.9 (1978); ***Gottschalk v. Benson***, 409 U.S. 63, 70 (1972); and ***Cochrane v. Deener***, 94 U.S. 780, 787-88 (1976)).

- **Regarding claim 37**, similarly to claim 24, the claim is also directed to non-statutory subject matter. Although the preamble of the claim recites *"a user equipment,"* the body of the claim does not positively recite any elements of hardware. The body of the claim recites *"means for obtaining access credentials," "means for sending the access credential," "means for establishing a secure tunnel," "means for receiving an internal IP address,"* and *"means for linking said access credentials with the inner IP address."* There is no further disclosure in the specification as to how the aforementioned "means for" are implemented. In light of discussions in the specification, *pars. 0023-0024 and 0065-0066 (accessing a local HTTP/non-HTTP services), par. 0048 (AAA protocol in accordance with IETF RFC 2865 protocol)*, it appears reasonable that said "means for" are be implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed subject matter is directed to non-statutory subject matter. The mere recitation of the machine in the preamble with an absence of a machine/hardware element in the body of the claim fails to make the claim statutory under 35 U.S.C 101. See

In re Comiskey, 499 F.3d 1365 (Fed. Cir. 2007); ***In Re Bilski***, 88 USPQ2d 1385; ***Diamond v. Diehr***, 450 U.S. 175, 184 (1981); ***Parker v. Flook***, 473 U.S. 584, 588 n.9 (1978); ***Gottschalk v. Benson***, 409 U.S. 63, 70 (1972); and ***Cochrane v. Deener***, 94 U.S. 780, 787-88 (1976)).

- **Regarding claims 25-27, 29-36, and 38-40**, claims 25-27, 29-36, and 38-40 are also directed to non-statutory subject matter for the same reasons.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 24-27 and 29-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- **Regarding claims 24-25, 27, 29, 32, and 35-40**, claims 24-25, 27, 29, 32, and 35-40 have been found in valid as indefinite because the claims recite "*means for*" languages and there is no structure disclosed in the specification. *"If there is no structure in the specification corresponding to the means-plus-function limitation in the claims, the claims will be found invalid as indefinite." Biomedino, LLC vs. Waters Technology Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007)

- **Regarding claims 26, 30-31, and 33-34**, claims 26, 30-31, and 33-34 are dependent on claim 24, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 24-27, 29-30, 37, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jin et al., (hereinafter "Jin"), U.S. Patent No. 6,643,782, issued on November 04, 2003, in view of Montenegro, U.S. Patent No. 6,571,289, issued on May 27, 2003.

- **Regarding claim 24**, Jin discloses an apparatus arranged for receiving a Single Sign-On service request in a telecommunication service network from a user via an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network *(col. 1, lines 15-21; the invention relates to a method for allowing single step log-on access to a network having more than one separate access area, such as a network divided into both public and private areas)*, the apparatus comprising:

means for receiving, at a Secure Service Entry Point of the service network, the access credentials from the user through the access network *(col. 4, lines 48-65; Fig. 1; the dial-up application prompts the user for user-name and password information, and contracts the NAS 2; see also col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client)*;

means for checking at the Secure Service Entry Point validity of the access credentials received from the user *(col. 4, lines 48-65; the NAS 2 prepares an access request packet containing the user-specified information as well as information about the NAS client 2 itself; see also col. 2, lines 23-30; the password entered by the user match the password specified in the account entry on the AAA database)*;

means for establishing a valid session with the user from the Secure Service Entry Point upon successful validity check of the access credentials *(col. 2, lines 44-46; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network; col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server,*

containing information regarding, for instance, the time at which the use's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database);

means for assigning an internal IP address between the Secure Service Entry Point and a Single Sign-On server to identify the user in the service network *(col. 2, lines 40-46; col. 5, lines 3-14; col. 5, lines 25-41; in order for the network to communicate with the user, the user must be assigned an IP address; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network; the NAS 2 assigns a genuine IP address to the user and logs the user on)*;

means for linking at the Single Sing-On server session data, access credentials and assigned internal IP address for the user *(col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the use's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database; the NAS 2 assigns a genuine IP address to the user and logs the user on)*; and

means for establishing a secure tunnel with from the Secure Service Entry Point the user when receiving the access credentials through the access network *(col. 2, lines 40-59; col. 5, lines 43-52; the SSG Server is inserted between the NAS and the AAA Server, and its function is to create secure channels to private areas of the network for authorized users)*; and by using the internal IP address assigned to identify the user in the service network *(col. 2, lines 40-46; col. 5, lines 3-14; col. 5, lines 25-41; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her*

session on the network; the NAS 2 assigns a genuine IP address to the user and logs the user on).

Jin does not explicitly disclose establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user; and using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic.

However, in an analogous art, Montenegro disclose a method for negotiating access to a private network for a mobile node including steps of establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user; and using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic *(Montenegro: col. 4, lines 14-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address source address of HA and a destination address of GW; the gateway will recognize that the MN has a 'binding' with a current address of FA; MN/CN is known as inner IP address and HA/GW is known as outer IP address; see also col. 3, lines 1-5 and lines 28-30; MN 110 receives an address from the private network 150; when it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150; the MN would be reachable via an IP address assigned by the ISP (FA 120); actual IP address, assigned by private network 150, is known as inner IP address and IP address, assigned by ISP, is known as outer IP address).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include the steps of establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user; and using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet *(Montenegro: col.2, lines 15-18)*.

- **Regarding claim 25**, Jin and Montenegro disclose the apparatus of claim 24.

Jin further discloses the Single Sign-On Server comprises means for generating service credentials for authorizing the user to access a service in the service network *(Jin: col. 1, lines 41-52; col. 2, lines 12-30; col. 5, lines 2-52)*.

- **Regarding claim 26**, Jin and Montenegro disclose the apparatus of claim 25.

Jin further discloses the service credentials are generated on a per service basis for the user upon service request *(Jin: col. 2, lines 28-30; the access-accept packet contains configuration data that enable the NAS to provide the desired service to the user)*.

- **Regarding claim 27**, Jin and Montenegro disclose the apparatus of claim 24.

Montenegro further discloses the Secure Service Entry Point comprises means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity *(Montenegro: col. 3, lines 31-65; the*

gateway 140 verifies an authentication which would accompany the registration request; the true home agent verifies the authentication for this registration and recognizes its validity).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet *(Montenegro: col.2, lines 15-18).*

- **Regarding claim 29**, Jin and Montenegro disclose the apparatus of claim 24.

Jin further discloses means for communicating the Secure Service Entry Point with the Single Sign-On Server *(Jin: col. 2, lines 52-59).*

- **Regarding claim 30**, Jin and Montenegro disclose the apparatus of claim 24.

Montenegro further discloses the Single Sign-On Server comprises means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point for *(Montenegro: col. 3, lines 15-54; the FA 120 is the recipient of the registration request and since it will not be allowed to complete the registration request itself, unless the ISP were somehow given secure access, to the private network 150, the request is forwarded to the gateway 140).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet *(Montenegro: col. 2, lines 15-18)*.

- **Regarding claim 37**, Jin teaches a user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication *(col. 1, lines 15-21)*, the user equipment, comprising:

means for obtaining access credentials from an Authentication Server of the core network as a result of being authenticated by the core network *(col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client)*;

means for sending the access credentials towards a Secure Service Entry Point the service network when accessing through the access network *(col. 2, lines 6-30; the AAA Server receives an access-request packet from an authorized NAS client; col. 4, lines 34-65)*;

means for establishing a secure tunnel with the Secure Service Entry Point of the service network through the access network, the secure tunnel *(col. 2, lines 40-59; col. 5, lines 43-52; the SSG Server is inserted between the NAS and the AAA Server, and its function is to create secure channels to private areas of the network for authorized users)*.

means for receiving an internal IP address assigned by the service network *(col. 2, lines 40-51; col. 5, lines 4-13 and 25-42)* and included as an [[inner]] IP address within the tunnelled traffic to identify the user in the service network *(col. 2, lines 40-51; col. 5, lines 4-13 and 25-42; the SSG server checks for an IP address in the access-reply packet; the SSG Server can log the user on with the IP address provided by the AAA Server and then forward the access-reply packet on to the NAS)*; and

means for linking said access credentials with the inner IP address and with the secure tunnel *(col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the user's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database)*.

Jin does not explicitly disclose establishing a secure tunnel making use an outer IP address assigned to the user by the access network for addressing the user; and included as an inner IP address within the tunnelled traffic to identify the user in the service network.

However, in an analogous art, Montenegro disclose a method for negotiating access to a private network for a mobile node including the steps of making use an outer IP address assigned to the user by the access network for addressing the user; and included as an inner IP address within the tunnelled traffic to identify the user in the service network *(col. 4, lines 14-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address source address of HA and a destination address of GW; the gateway will recognize that the MN has a*

'binding' with a current address of FA; MN/CN is known as inner IP address and HA/GW is known as outer IP address; see also col. 3, lines 1-5 and lines 28-30; MN 110 receives an address from the private network 150; when it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150; the MN would be reachable via an IP address assigned by the ISP (FA 120); actual IP address, assigned by private network 150, is known as inner IP address and IP address, assigned by ISP, is known as outer IP address).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include steps of making use an outer IP address assigned to the user by the access network for addressing the user to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet *(Montenegro: col.2, lines 15-18).*

- **Regarding claim 41**, Jin discloses a method for supporting Single Sign-On services in a telecommunication service network for a user accessing said service network through an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network *(col. 1, lines 15-21; the invention relates to a method for allowing single step log-on access to a network having more than one separate access area, such as a network divided into both public and private areas)*, the method comprising the steps of:

receiving at the service network the access credentials from the user through the access network *(col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client)*;

checking validity of the access credentials received at the service network, establishing a valid session with the user upon successful validity check of the access credentials *(col. 2, lines 23-30; the password entered by the user match the password specified in the account entry on the AAA database)*;

assigning at the service network an internal IP address for the user to identify the user when accessing a service in the service network *(col. 2, lines 40-46; col. 5, lines 3-7; in order for the network to communicate with the user, the user must be assigned an IP address; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network)*;

linking session data, access credentials and the assigned internal IP address for the user at an entity of the service network *(col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the user's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database)*;

linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side *(col. 1, line 65-67 to col. 2, lines 1-9)*.

Jin does not explicitly disclose establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an

outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network.

However, in an analogous art, Montenegro disclose a method for negotiating access to a private network for a mobile node including steps of establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network *(col. 4, lines 14-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address source address of HA and a destination address of GW; the gateway will recognize that the MN has a 'binding' with a current address of FA; MN/CN is known as inner IP address and HA/GW is known as outer IP address; see also col. 3, lines 1-5 and lines 28-30; MN 110 receives an address from the private network 150; when it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150; the MN would be reachable via an IP address assigned by the ISP (FA 120); actual IP address, assigned by private network 150, is known as inner IP address and IP address, assigned by ISP, is known as outer IP address)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include steps of establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP

address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet *(Montenegro: col.2, lines 15-18)*.

- **Regarding claims 42-44**, claim 42-44 are similar in scope to claims 25-27 respectively, and are therefore rejected under similar rationale.

- **Regarding claim 45**, Jin and Montenegro disclose the method of claim 41.

Jin and Montenegro further disclose the step of linking session data, access credentials and assigned internal IP address for the user *(Jin: col. 2, lines 40-51; col. 5, lines 25-42)* further includes a step of communicating a first device named Secure Service Entry Point in charge of the secure tunnel with a second device named Single Sign On Server where the step of linking takes places *(Jin: col. 2, lines 40-51; col. 5, lines 25-42; Montenegro: col. 4, lines 14-53)*.

Claims 31-36, 38-40, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jin and Montenegro, as applied to claims 24 and 41 above, and further in view of Schneider et al., (hereinafter "Schneider"), U.S. Patent No. 6,105,027, issued on August 15, 2000.

- **Regarding claim 31**, Jin and Montenegro disclose the apparatus of claim 24.

Jin and Montenegro do not explicitly disclose when the user is accessing a local HTTP service, or an external service in a network different than the currently accessed

service network, wherein the Single Sign-On Server further comprises means for checking whether the user had been previously authenticated or not.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein when the user is accessing a local HTTP service *(col. 43, lines 16-24; col. 45, lines 54-60; once the proxy has confirmed that access is to be allowed to the information resource specified in the message, the proxy originates a new session to the actual server, the HTTP service on server 407)*, or an external service in a network different than the currently accessed service network, wherein the Single Sign-On Server further comprises means for checking whether the user had been previously authenticated or not *(Schneider: col. 48, lines 10-19; the other access filters between the user and the information item need only determine whether the request has already been authenticated by another access filter)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro to include means for checking whether the user had been previously authenticated or not in order to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 32**, Jin, Montenegro, and Schneider disclose the apparatus of claim 31.

Schneider further discloses the Secure Service Entry Point comprises means for communicating with an intermediate entity arranged to intercept the user's access to the

HTTP local service, or to the external service in an external network *(Schneider: col. 26, lines 37-39; col. 40, lines 61-66; the service proxies intercept traffic for service such as the World Wide Web and do access checking on the traffic).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro to include means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20).*

- **Regarding claim 33**, Jin, Montenegro, and Schneider disclose the apparatus of claim 32.

Schneider further discloses the intermediate entity is an HTTP-proxy *(Schneider: col. 40, lines 60-67; col. 3, lines 59-67).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein the intermediate entity is an HTTP-proxy to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20).*

- **Regarding claim 34**, Jin, Montenegro, and Schneider disclose the apparatus of claim 32.

Schneider further discloses intermediate entity is a firewall *(Schneider: col. 3, lines 59-67; access checking at the application is usually done in the firewall by proxies)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein intermediate entity is a firewall to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 35**, Jin and Montenegro disclose the apparatus of claim 24.

Jin and Montenegro do not disclose when the user is accessing a non-HTTP local service, wherein the Single Sign-On Server comprises means for checking whether the user had been previously authenticated or not.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein the Single Sign-On Server comprises means for checking whether the user had been previously authenticated or not *(Schneider: col. 48, lines 10-19; the other access filters between the user and the information item need only determine whether the request has already been authenticated by another access filter)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and

method of Jin and Montenegro, to include means for checking whether the user had been previously authenticated or not in order to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 36**, Jin and Montenegro disclose the apparatus of claim 24.

Jin further discloses the means for receiving access credentials at the Secure Service Entry Point *(Jin: col. 4, lines 48-65; Fig. 1; the dial-up application prompts the user for user-name and password information, and contracts the NAS 2; see also col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client)*.

Jun and Montenegro do not explicitly disclose comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, including means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user *(Schneider: col. 6, lines 12-16; col. 10, lines 11-54)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is

present to indicate a successful authentication of the user to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 38**, Jin and Montenegro disclose the user equipment of claim 37.

Jin further discloses the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network *(Jin: col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client)*; means for generating and returning an authentication response to the core network *(Jin: col. 2, lines 16-39; if the passwords match, and all the other requirements are met, then the AAA Server send the NAS an "access-accept" packet in response; if nay requirement is not met, then the AAA Server responds with a "access-reject" packet)*;

Jin and Montenegro do not explicitly disclose means for generating a public and private key pair; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising means for generating a public and private key pair *(Schneider: col. 10, lines 19-27 and 59-61)*; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network *(Schneider: col. 10, lines 19-27 and 59-61)*;

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, to include means for generating a public and private key pair; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20).*

- **Regarding claim 39**, Jin and Montenegro disclose the user equipment of claim 37.

Jin further discloses the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network *(Jin: col. 1, lines 65-67 to col. 2, lines 1-9)*; means for generating and returning an authentication response to the core network *(Jin: col. 1, lines 65-67 to col. 2, lines 1-9)*;

Jin and Montenegro do not explicitly disclose means for requesting a digital certificate obtainable from the core network.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising means for requesting a digital certificate obtainable from the core network *(Schneider: col. 6, lines 12-17; col. 10, lines 11-42)*;

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and

method of Jin and Montenegro to include means for requesting a digital certificate obtainable from the core network to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 40**, Jin and Montenegro disclose the user equipment of claim 39.

Jin and Montenegro do not explicitly disclose the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable *(Schneider: col. 10, lines 11-54)*;

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro to include the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters *(Schneider: col. 5, lines 66-67 to col. 6, lines 1-20)*.

- **Regarding claim 46**, claim 46 is similar scope to claim 31, and is therefore rejected under similar rationale.

(10) Response to Argument

1. Rejection of Claims 24-27 and 29-40 under 35 U.S.C. § 101 / § 112:

a) Appellant argues that *"[n]ot only do the claim preambles limit the claims to an apparatus, but such 'means for' elements are statutorily authorized under § 112, ¶6;"* and *"the means necessary to carry out the recited claim functions using the telecommunications nodes and elements clearly depicted in the figures and described with the reference thereto."*.

The Examiner respectfully disagrees with the Appellant.

The Examiner respectfully submits that one of ordinary skill in the art would understand that communication between client and server via the Internet/network is performed by a web browser installed on client device and web applications/services embedded on the server. Web browser and web applications, which are implemented in software, provide means for performing authentication and establishing secure communication session between client and server. User is able to access to a web server using either a desktop computer, laptop, PDA, or even cell phone as long as an appropriate web browser is installed. The Examiner respectfully submits that claimed functions are performed by web browser, which is software installed on the telecommunications nodes and not by 'the telecommunication node' itself as argued by the Appellant. Regarding the claim language, although the preamble of the claim 24 recites *"an apparatus,"* the body of the claim does not positively recite any elements of hardware. The body of claim recites *"means for receiving the access credential," "means for checking validity of the access*

credential, "means for establishing a valid session," "means for assigning an internal IP address" "means for linking," and *"means for establishing a secure channel."* There is no further disclosure in the specification as to how the aforementioned "means for" are implemented. In light of discussions in the specification, *pars. 0023-0024 and 0065-0066 (accessing a local HTTP/non-HTTP services), par. 0048 (AAA protocol in accordance with IETF RFC 2865 protocol)*, it appears reasonable that said "means for" are implemented by software by one of ordinary skill in the art at the time the invention was made. Therefore, the claimed subject matter is directed to non-statutory subject matter. The mere recitation of the machine in the preamble with an absence of a machine/hardware element in the body of the claim fails to make the claim statutory under 35 U.S.C 101.

2. Rejection of Claims 24-27, 29-30, 37, and 41-45, under 35 U.S.C. § 103(a):

a) Appellant argues that *"the Examiner did not provide any substantive response to the arguments present by Applicants in response to the prior office action."*

The Examiner respectfully disagrees with the Appellant.

The Examiner respectfully submits that the Office Action mailed on 02/18/2009 designates four pages for response to Appellant's arguments *(pages 2-6)*. In case the Examiner has missed any of the Appellant's arguments, it is respectfully requested that the Appellant particularly point out which arguments the Examiner has not provided a response to so that the Examiner could address them accordingly.

b) Appellant argues that *"Montenegro thus fails to anticipate two different IP addresses corresponding to the same entity accompanying the packet and used to different purposed."*

The Examiner respectfully disagrees with the Appellant.

The Examiner respectfully submits that Montenegro does disclose two different IP addresses corresponding to the same entity accompanying the packet and used to different purposed *(col. 3, lines 1-5 and lines 28-30; MN 110 receives an address from the private network 150; when it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150; the MN would be reachable via an IP address assigned by the ISP (FA 120); [i.e., there are two different IP addresses corresponding to the same MN 110; one is used when MN is in private network and another one is used when it roams and connects to FA 120]; see also col. 4, lines 14-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address source address of HA and a destination address of GW; the gateway will recognize that the MN has a 'binding' with a current address of FA)*. In addition to the above, it is noted, however, that the features upon which applicant rely *(i.e., "two different IP address corresponding to the same entity accompanying the packet and used for different purpose")* are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

c) Appellant argues that *"Montenegro fails to disclose an outer IP address assigned to the user by the access network for addressing the user and an internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic."*

The Examiner respectfully disagrees with the Appellant.

Montenegro does disclose an outer IP address assigned to the user by the access network for addressing the user and an internal IP address assigned to identify the user in the service network as an inner IP address in the tunneled traffic *(col. 4, lines 14-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address source address of HA and a destination address of GW; the gateway will recognize that the MN has a 'binding' with a current address of FA; MN/CN is known as inner IP address and HA/GW is known as outer IP address; see also col. 3, lines 1-5 and lines 28-30; MN 110 receives an address from the private network 150; when it moves, its actual IP address will no longer be the same as when the MN 110 resided in the private network 150; the MN would be reachable via an IP address assigned by the ISP (FA 120); actual IP address, assigned by private network 150, is known as inner IP address and IP address, assigned by ISP, is known as outer IP address).*

(11) Related Proceedings Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Conclusion

For the above reasons, it is believed that the rejection should be sustained.

Respectfully submitted,

Luu Pham

/Luu Pham/

Examiner, Art Unit 2437

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437